韓國 컴퓨터情報學會 論文誌
第8卷 第3號, 2003. 9.

2003-8-3-2-6

ATM 방화벽 스위치 기반의 패킷 보안에 관한 연구

임 청 규*

A Study on Packet Security of ATM Firewall Switch

Chung-Kyu, Lim*

요 약

ATM 망은 개방형 통신망에서 다양한 서비스 와 QOS를 지원하며 대역폭 확장을 통한 망 자원의 효율성과 융통성을 제공한다. 그러나 이런 트래픽 들에 대한 품질 서비스에 대한 연구가 많이 진행되고 있으나 트래픽 보안을 안전성 검사는 연구대상 부분이 많이 존재한다. 본 논문에서는 ATM FORUM 보안그룹에서 정한 ATM Security Specification 1.1 중심으로 보안서비스 개념을 소개하고 외부망에서 내부망으로 들어오는 패킷들을 보안을 위한 안정성기준으로 효율적으로 처리하는 스위치와 결합한 방화벽처리 루틴 및 CAC 루틴을 소개한다. 패킷들의 안전성 등급을 분류처리 하기 위하여 SSC(Special Service Cell)를 도입한다. 본 논문에서는 스위치 처리량, 셀 지연등을 위한 시뮬레이션 시나리오을 제안한다.

Abstract

This paper presents the design of a value-added ATM switch. The ATM switch ca perform CAC Processing and Firewall Processing Routine at packet-level (IP) at the ATM environment per port. The proposed two routine are integrated into the components of ATM switch. The Firewall switch employs a suggested two routine model to avoid or reduce the latency caused by filtering. Also, we suggest four classes are defined, namely, classes A, B, C, and D, which are orded from the safest to the most dangerous. The suggested model performance of ATM Firewall switch is estimated simulation in terms of the throught and latency by computer .

▸ Keywords : 방화벽(Firewall), 패킷(Packet), 보안(Security), 트래픽(Traffic)

* 전북과학대학 인터넷정보계열 조교수

Ⅰ. 서 론

초고속 정보화 사회의 기반은 고품질의 멀티미디어를 전송할 수 있는 광대역 종합정보통신망(B-ISDN : Broadband-Integrated Services Digital Network)이다. 이와 같은 멀티미디어를 전송할 수 있는 정보통신망의 구축은 필수적이라 할 수 있다. 정보 통신이 사회 생활, 직장 생활, 여가 생활 등 여러 방면에 두루 사용되어짐에 따라 사용자의 요구도 다양한 형태로 분출되고 있다. 사무 자동화, 공장 자동화, 인터넷 보급 등에 따라 LAN간 접속, 대용량 파일 전송, 고속 CAD/CAM, 고속 팩스 등의 고속 데이터 통신과 아울러 화상 회의, 화상 전화, HDTV, VOD, CATV 등의 음성과 영상 통신이 복합된 멀티미디어 정보통신이 요구되고 있다[1]. 미래 통신은 기존의 단일 미디어 통신에서 음성, 데이터, 영상 등이 혼합되는 멀티미디어 통신이 주체가 될 것이다.

이러한 다양한 종류의 통신 서비스를 제공할 수 있는 멀티미디어 정보통신망을 효율적으로 구축하기 위해서 1988년 ITU-T는 B-ISDN을 구성하기 위한 기본 통신 방식으로 비동기식 전달 모드(ATM : Asynchronous Transfer Mode)를 채택하였다[2-7].

ATM 망에서는 전송하고자 하는 정보를 53바이트 고정 길이의 패킷인 셀을 분할 또는 조립하여 여러 정보원으로부터 발생되는 셀을 보낼 필요가 있을 때에만 통계적 다중화(Statistical Multiplexing) 하여 전송하며 패킷 헤더 부분에 목적지 정보를 부가하여 고정 크기의 셀 형태로 전달된 후 원래의 정보로 복원하는 방식이다.

이와 같이 모든 사용자 정보를 고정 크기의 셀 단위로 처리하여 하드웨어로 셀 전송이 이루어지기 때문에 저속에서 고속까지의 다양한 서비스를 제공할 수 있다. 이렇게 다양한 종류의 서비스를 제공할 수 있는 ATM 전송은 다음과 같은 장점들을 갖고 있다.

첫째, 현존하는 서비스와 미래에 나타날 서비스를 지원하기 위한 융통성 확보가 용이하다. 둘째로는 셀 단위로 전송을 수행하기 때문에 동적인 대역폭 할당이 가능하다. 셋째로는 모든 정보 형태를 통합하여 전달 할 수 있다.

그러나 ATM 의 이러한 장점에도 불구하고 컴퓨터 통신을 이용한 해커(Hacker)와 크래커(Cracker) 에 의한 각종 정보 손실에 대한 위협이 커졌다. 특히 ATM 망에서는 짧은 시간에 많은 자료를 해킹 및 크래킹을 할 수 있어 그에 대한 보안이 더욱 중요시되었다. ATM 망에서는 이러한 보안의 중요성 때문에 1995년 ATM Forum에서 보안 문제에 대한 공식적인 연구가 있었으나 기존 서비스와 연관성으로 인해 1998년에 ATM Security Version 1.0이 완성되었고 2001년에는 ATM Security Specification Version 1.1 이 나오게 되었다. ATM 망은 통신 매체 및 망의 성능이 향상되어 대량 및 초고속 버스트 트래픽을 전송 하는데 보안 문제가 크게 대두되었다[8].

본 논문의 구성은 제 2장에서는 ATM망에서 요구하는 보안에 대한 요구사항을 개략적으로 분석하고 ATM 망에서 연동해서 운영되는 ATM 스위치의 보안을 위한 논리적인 설계를 제시 하였다[9]. 제 3장에서는 ATM siwtch 보안을 위한 패킷 기반의 CAC 처리 루틴 과 방화벽 처리 루틴을 수행하는 제안 모델 의 구조 및 동작에 대하여 살펴본다. 제 4 장에서는 시뮬레이션 시나리오상의 수학적 분석과 환경을 서술하고 있다. 마지막으로 제 5장에서는 본 논문의 결론으로 제안된 모델을 분석하고하고 향후 추가 연구 및 응용 방향을 제시하였다.

Ⅱ. ATM 망의 보안 서비스와 종류

초고속 멀티미디어 서비스를 수행할 수 있는 ATM 망에서의 보안 요구 사항을 ATM Forum 1.1을 토대로 소개한다.

1. ATM 보안 서비스

ATM Forum의 보안 표준 1.1 에 따르면 보안 요구사항을 다음과 같다.

① 정보 기밀성(Information Confidentiality)

정보 기밀성은 권한이 없는 사용자로부터 데이터의 보안을 위한 것으로 암호기술을 제공한다. ATM 망은 AAL 레벨 보다 셀 레벨에서의 기밀성 서비스를 제공하며 고정된 길이의 셀를 사용하므로 효율적인 암호화를 허용한다. 더욱이 셀의 Payload 만이 암호화가 되고 중간 Hop 노드에서

는 복호화가 없이 망에 의해 전달 될 수 있다. 이 서비스는 대칭형 암호화 알고리즘을 사용한다. 대칭형 알고리즘은 스피드, 블록 크기 및 보안 성질 등 때문에 ATM 셀 암호화를 위해서 사용한다.

② 정보 무결성(Information Integrity Service)

정보 무결성 서비스는 사용자들 간에 서로 정보를 주고받데 정보의 값 및 전송 순서 수정되지 않았음을 검증한다.

③ 정보 인증(Information Authentication)

정보의 발신자와 수신자의 신분을 확인하는 보안 서비스다. 이 서비스는 침입 또는 스푸핑 위협으로부터의 방어를 제공한다. 이는 안전한 연결 제공, 키 교환 서비스 및 보안 협상 파라미터의 안전한 교환 등의 보안 서비스 실현에 필수적이다. 인증 서비스는 통신하는 양자 간 또는 단 방향 등 형태로 진행된다.

④ 부인 방지(Non-repudiation Services)

이 서비스는 사용자가 정보 서비스 와 자원에 대한 접근했음을 부인하는 것을 방지 하는 것이다.

2. ATM 보안 위협 종류

ATM 망은 테스트, 이미지, 음성 및 비디오 등의 결합 메시지를 전송한다. 다른 망과는 달리 ATM 망은 다음과 같은 위협요소를 가지고 있다.

① 도용

도용 위협은 메시지 전송자가 불법적인 권한을 가지고 데이터 또는 시설을 이용하는 것을 의미한다.

② 메시지 순서

메시지 순서 위협은 메시지 전체 또는 일부가 반복되거나, 시간변화, 또는 재순서 배열 등이 일어날 때 발생한다. 이는 인증정보를 활용하는데 사용된다.

③ 정보 수정

수신정보, 라우팅 정보, 및 기타 관리 정보 등이 손실 또는 수정되는 것을 의미한다.

④ 서비스 부인

서비스 부인은 메시지 기능 수행을 방해해서 접근 부인, 통신 방해 등을 유발한다. 즉 법적인 사용자가 서비스를 이용 할 수 없도록 한다. IP 주소 서비스 부인위협과 대역폭 선점에 의한 위협이 있다. IP 주소 선점에 의한 위협은 사용하지 않는 IP 주소를 할당하여 IP 주소를 할당받지 못하도록 하는 것이다. 대역폭 선점에 의한 위협은 우선순위가 높은 트래픽을 모든 대역폭에 서비스함으로서 서비스 부인을 유발하는 위협이다.

⑤ 거절

거절 위협은 메시지 전송자 또는 수신자가 메시지 전송, 수신 등을 거부하는 것이다. 이는 송신자 부인, 전송 부인, 수신자 부인 등을 포함한다.

⑥ 정보 노출

정보 누출은 트래픽 전송을 모니터링 하여 불법적인 자가 정보를 획득하거나 저장되어 있는 메시지를 불법적으로 접근하는 위협현상이다. 정보가 전송·수신 할 때에 전송 및 수신 경로가 변경되므로 발생한다.

⑦ IP 스푸핑

불법적인 접근권한을 가진 자는 서버의 ATM 주소를 알아내어 해당 호스트에 접속을 시도하여 조작된 IP 주소를 등록함으로 써 발생한다. 조작된 IP 주소를 이용하여 패킷을 전송한다. 공격당한 IP 주소로 보내는 모든 정보는 불법적인 접근자에게 전송된다. 이 위협은 ATM 망에서 감지하기 어려운 것이다.

III. 제안된 ATM 스위치 모델

본 장에서는 제안된 ATM의 방화벽 스위치 모델을 제안하고 이 모델을 기반으로 성능 분석을 위한 방화벽 패킷 처리 루틴을 프로우 차트와 함께 제시하였다.

1. 제안된 방화벽 스위치의 모델

ATM망에서 요구하는 보안 서비스를 시뮬레이션 하기 위하여 스위치 개념을 일부 수정하여 모델을 제시한다.

ATM 스위치 구성은 일반적으로 다음과 같은 기능으로 구성한다.

① LI

SDH 프레임 형태의 페이로드로부터 셀을 축출하여 각 셀을 목적 포트를 결정하고 ATM 망의 스위치로 보내고 셀에 부착된 내부 태그에 기록한다. 입력된 셀들은 라우팅 과정, CAC 처리 루틴 및 방화벽 처리 루틴등을 수행한다.

② CAC

호 접수 및 시그널링 메시지를 처리하며 신호 메시지에 따라 망 자원을 안전한 관리를 위한 호 설정 및 대역폭 할당등의 Call 서비스 구현을 위한 향상된 기능을 제공한다.

③ 설프 라우팅 스위치

스위치 네트워크에서는 입력단에서 들어온 패킷들의 정보에 따라 셀들을 라우팅하거나 셀 헤더에 부착된 방화벽 관련 정보에 따라 셀을 방화벽 처리 루틴으로 보내어 보안을 위한 안전성 검사를 거친 후에 스위치 출력단으로 보낸다.

④ 방화벽 처리 루틴

제안된 각 셀에 부착된 내부 방화벽 관련 정보를 처리하는데 안전한 셀은 스위치 출력단으로 보내게 되고 그렇지 않으면 셀을 제거한다. 이 방화벽 처리 과정은 셀 필터링 서비스 기능을 제공한다. 이 방화벽 처리 루틴은 IP 레벨 보안 기법을 제공하며 ATM 스위치의 하드웨어 요소로 합병한다. 대부분 셀 필터링서비스는 병렬적으로 정상적인 셀 처리로 수행되며 대부분 비용이 ATM 스위치의 기본비용에 포함된다.

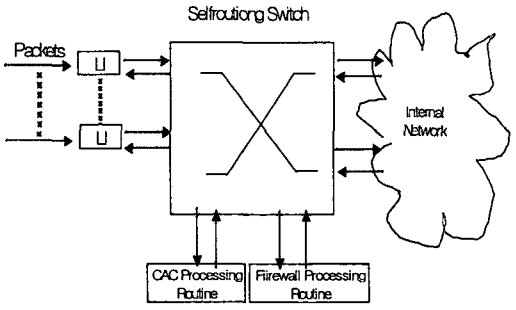

그림1. ATM 스위치 구성
Figure 1. ATM Switch Configuration

2. 패킷 처리 과정

〈그림 1〉과 같이 외부 망으로부터 패킷 들이 어떻게 들어오는지를 알 수 있다. 외부 망에서 내부 망으로 들어오는 패킷들을 처리한다.

각 패킷 획득과 일련의 패킷 처리 과정을 통해서 패킷의 안전성 여부를 판단한다. CAC 처리 과정과 방화벽 처리과정을 통한 검사과정이 끝나면 해당 패킷은 안전함을 의미하므로 스위치의 출력 포트로 보낸다. 그렇지 않으면 안전하지 않은 패킷이므로 방화벽 처리 루틴으로 보내어 드롭 시킨다. 그림2는 일련의 패킷 처리 과정을 플로우차트로 나타낸 것이다.

〈그림 2〉는 패킷 처리 과정으로 일련의 다음 단계로 분류한다.

① 타당한 패킷의 형태를 분류한다. 어떤 형태의 패킷이든 법적인지를 조사한다.

② 들어오는 패킷이 패킷 필터링 과정을 통해서 CRC 메시지 타입의 비안전성 패킷이면 CRC 패킷 처리 루틴으로 보내어 조사를 하고 그렇지 않고 공격용 패킷이면 방화벽 패킷 필터링 처리 루틴으로 보낸다.

③ CRC 메시지 성의 패킷이 아니고 일반 패킷이면 방화벽 패킷 필터링과정으로 보내어 검사를 실시한다.

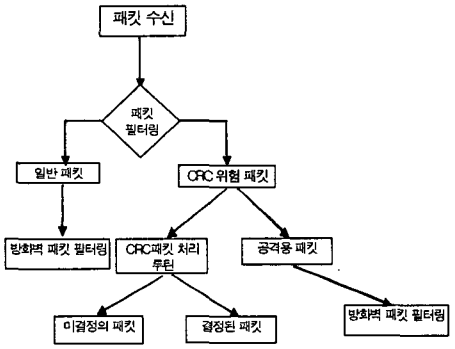

그림 2. 패킷 처리과정
Figure 2. Packet Processing Routine

3. 방화벽 패킷 처리 과정

방화벽은 많은 양의 데이터를 고속으로 전송하는데 안전성을 보장하여야 한다. 고속의 스위치와 결합을 해서 이 안전성 여부를 점검하는데 패킷 지연 현상을 초래 할 수 있다. 하지만 외부 망에서 들어오는 패킷들의 안전성 점검은 신뢰성 보장에 중요하다. 이를 위해서 다음과 같은 논리 구조를 제안해서 이를 방화벽 처리 루틴에서 사용한다.

ATM Cell Header	Security Cell Field	Payload Type	Length	PayLoad	CRC

그림3. 보안 서비스 셀의 논리 구조
Figure 3. Logical structure of Security Service Cell

방화벽 처리 루틴에서 이루어지는 무결성 검사 와 암호화는 ATM 계층을 통해서 수행한다. 보안관점에서 볼때 방화벽은 외부의 ATM 망에서 터널을 구현한다. CRC 메시지 타입과 데이터 셀을 보이지 않게 할 수 있다.

방화벽 관리 평면의 변화는 이들 터널을 설정, 관리, 해제 할 수 있다. ATM 보안 서부 레이어는 SAAL 로부터 들어오는 패킷과 메시지를 통해서 연결이 설정되었는지 않다. 그 다은 해당 방화벽 처리 루틴으로 하여금 보안 서비스를 실행하는데 이 셀을 보안 서비스 셀(SSC) 이라 한다. ATM 계층으로부터 보안 서부 계층는 이 보안 서비스 셀을 조절하는데 이 방화벽에서 이 서부 레이어를 인코드하여 이 셀을 만들어낸다. 방화벽으로부터 SSC을 관리해야하며 ATM 계층의 보안 서부레이어는 SSC를 처리해야 한다. SSC는 셀 레벨에서 수송되고 확인된다. 이를 위한 SSC를 사용자 데이터(디지탈 서명, 타임 스탬프등)에 관련한 데이터를 수송한다. SSC를 데이터 셀 사이에 삽입된다. 데이터와 SSC 사이의 동기화는 발생하지 않을 것이다.

두 형태의 셀은 같은 VPI/VCI Pair 상에서 전달되며 망으로부터 같은 정책을 따른다. 투명성 문제를 해결 할 수 있다. 이유는 중간 망에서 ATM 스위치의 프로토콜을 변화시킬 필요 없다. SSC는 방화벽에 의해서 인식되어 간다. 방화벽은 SSC 의 보안 셀 필드 와 SSC 의 페이로드 에 위치한 CRC 코드에 중심이 된다. 페이로드 타입은 셀 안의 명시된 필드에 중심이 된다. 셀 필드, CRC 생성, 제어는 하드웨어로 구현 될 수 있다. 그러나 디레이를 초래한다. 삽입 된 셀로 인한 밴드위드스는 전송자 터미날에서 요구한 것 보다 높을 것이다. SSC는 더 많은 보안 서비스의 유형을 제공 할 수 있다. 이 방식에서는 데이터 셀 사이에 SSC를 삽입한다. SSC 의기능 는 인증, 키 교환, 동기화, 상태 정보등을 수행한다. SSC이 삽입된 후의 데이터 셀의 수는 QoS 파라미터에 따른다. 데이터 실제 Bit Rate는 실제 다를 수 있다. 데이터 셀이 도착하면 요구된 SSC 이 수신 된 후에 인증의 타당성을 점검한다. 만약에 에러가 발생하면 방화벽은 비안전성 패킷을 드롭 시키거나 연결을 종료하면서 경고 메시지를 보내고 관리자에 의해 요구된 행동을 취할 수 있다.

Ⅳ. 시뮬레이션 및 성능분석

1. 방화벽 스위치 의 처리량

시뮬레이션 환경에서 방화벽 스위치 의 Throughput 는 다음과 같은 식으로 표현된다.

$$THR = \frac{STHR * CN}{DR}$$

DR 은 트래픽 부하의 방화벽 의 폐기률, CN는 트래픽 부하가 구성하고 있는 셀의 수, THR는 CRC 처리 및 방화벽처리 의 처리량 이다. CN는 트래픽 샘플로 측정가능하고 THR은 전통적인 IP 방화벽 처리 에이타를 사용하여 측정한다. 트래픽 흐름의 첫 번째 패킷이 방화벽에 도착 할때 두개의 루틴 과정에서 검사 받는다.

2. 방화벽 스위치의 지연

본 절에서 방화벽 패킷 처리 루틴에 의한 지연을 회피하고 줄이는 효과에 대해 증명한다. 다음의 시나리오를 생각하자. 링크의 전체용량을 C (ceels/sec) 라 하고 평균 밴드위드스 의 연결하에 가정하고 어떻게 지연되는지 알아본다.

- $P_r(DE=0)$: 패킷에 의해서 어떤 지연이 발생하지 않을 확률이다. 이 확률은 방화벽의 패킥 처리는 짧은 시간이기 때문에 0이다.
- $EXP[DE]$: 패킷 처리 루틴에 의해서 사용되는 경우에 패킷에 의해 발생하는 평균 지연이다. 서로 다른 연결들 사이의 셀은 완전히 서로 사이사이로 입력된다고 하자. 각 셀 슬롯 중에 들어오는 셀이 연결 중에 속할 확률 λ 는 $\lambda = B/C$ 로 표현된다. T를 연결 중에 두 개의 연속 적인 셀들 사이의 도착 간격이라 하자 그러면

  $Pr[T=i]=\lambda(1-\lambda)^{i-1} : i=1,2,3,...,\lambda=B/C$. λ 가 작다면 기하학적 이산 분포는 지수 분포를 따른다고 볼 수 있다. 지수 분포는 $Pr(T > t) = \epsilon^{-\lambda t}$ 이다.

  그리고 N 은 포아송 (poisson distribution) 분포를 따르다. 만약에 L-2미만의 셀이 타임 윈도우 (0,R] 구간에 도착한다면 패킷에 의해 경험하는 어 떤 지연 발생이 없다.

  $T^{\wedge}$ 는 첫 번째 셀의 도착 시간이 0 이라고 가정 했을 때 L^{th} 셀의 도착 시간이다. $T^{\wedge}$ 의 밀도 함수는

  $$f_T(t) = f_{ER_{L-1,\lambda}}(t) = \frac{\lambda^{L-1} t^{L-2} \epsilon^{-\lambda t}}{(L-2)!}$$

  $ER_{n,\lambda}$ 는 어랑 임의 변수이다.

3. 실험 결과

본 절에서는 인터넷 트래픽으로부터 측정된 매개변수를 적용한 방화벽 스위치 성능의 수치 결과를 계산한다. 방화벽 스위치의 대역폭 분류에 따른 처리량과 셀 지연 의 정량적인 측정으로 한다. 셀 지연은 다음과 같이 나타나는데 셀 발생은설 명한대로 아래와과 같이 Poisson 분포를 따르도록 하였다.

$$\Pr(\text{T시간동안에 k개 도착}) = \frac{(\lambda T)^k}{k!} e^{-\lambda T} \quad \lambda : \text{입력 부하}$$

다음의 결과는 각 부하량에 따른 평균 셀 지연을 나타낸 것이다.

테이블 1 : 각 부하량에 따른 평균 셀 지연
Table 1. Mean Cell Latency Under Different Load

	Mean Delay(50)	Mean Delay(70)	Mean Delay(80)	Mean Delay(95)
0.25 M	2.80E-05	5.51E-05	4.66E-05	6.68E-05
0.5M	1.46E-05	2.50E-05	2.24E-05	3.70E-05
1M	9.02E-06	2.37E-05	1.26E-05	1.52E-05
2M	7.94E-06	1.11E-05	1.08E-05	1.28E-05
4M	7.21E-06	1.04E-05	1.11E-05	7.63E-06
8M	6.43E-06	7.09E-06	1.11E-05	7.69E-06
10M	5.56E-06	6.57E-06	1.01E-05	7.68E-06

V. 결 론

본 논문에서는 외부 망에서 수신되는 패킷 중심의 트래픽을 검사하여 보안서비스 등급을 향상시키는 모델을 제안하고 이를 위하여 방화벽 처리 및 CAC 처리 루틴을 경유하도록 하였다. CAC 처리루틴은 호설정과정에서의 보안성을 향상하는 것이고 방화벽 처리 루틴은 보안등급 별로 분류하여 제공하는 패킷 감시 처리기로 본다. 방화벽 처리 루틴중심의 스위치는 ATM 스위치 의 하드웨어 요소로 패킷 보안 기법을 포함한다. 그리고 패킷 필터링 운영 대부분이 정상적인 셀 처리로 병렬적으로 수행되며 그의 비용은 ATM 스위치의 기본비용으로 흡수된다. 제안한 스위치는 패킷 필터링에 의해서 일어나는 실험 결과 같이 지연(latency)을 줄여준다.

그리고 처리량 과 지연측면에서 성능 분석시나리오를 제공하였다. 마지막으로 미해결된 MPOA에서 보안 역할 뿐만 아니라 방화벽 스위치에 대한 심층 연구 및 보안등급별 패킷을 적용한 경우에 각 부하량에 따른 셀과 지연 관계에 때한 연구 분석이 필요하다.

참고문헌

[1] L. Zhang, "Virtual clock: a new traffic control algorithm for packet switching," ACM Trans. Computer Systems, 9(2):101-124, May 1991.

[2] Katevenis, M., Sidiropoulos, S., and Courcoubetis, C, "Weighted round-robin cell multiplexing in a general purpose ATM switch chip," IEEE J. Sel Areas Commun., SAC-9, pp. 1265-1279, 1991.

[3] Biao Chen, Gopal Agrawal, and Wei Zhao. Optimal synchronous capacity allocation for hard real-time communications with the timed token protocol. In Proc. of the 13th Real-Time Systems Symposium, pages 198-207, Phoenix, Arizona, December 1992.

[4] Abhay K, Parekh and Robert G. Gallager, "A generalized processor sharing approach to flow control in integrated services networks: The single-node case," IEEE/ACM Trans. on Networking, 1(3):344-357, June 1993.

[5] S. Jamaloddin Golestani, "A self-clocked fair queueing scheme for broadband applications," In Proc. IEEE INFOCOM'94, pages 636-646. IEEE, 1994.

[6] T. Wang, T. Lin, and K. Gan, "An Improved Scheduling Algorithm for Weighted Round-Robin Cell Multiplexing in an ATM Switch," Proc. ICC'94, Vol. 2, pp. 1032-1037, 1994.

[7] S. Sathaye, "ATM Forum Traffic Management Specification, Version 4.0," ATM Forum Technical Committee, Mar. 1996.
[8] Thomas Tarman, "ATM security Framework 1.0,". ATM Forum Technical Committee, Mar. 2001.
[9] Jun XU and MUKESH SSINGHAL, "Design of a High-Performance ATM Firewall," ACM Transactions on Information and System Security, Vol.2, No. 3, Pages 269-294, August 1999.

저 자 소 개

임 청 규

1986 한남대학교 전자 계산공학과 졸업
1990 自由中國 (臺灣) 國立交通大學校 資訊情報工學科 工學碩士
1998 국립 전북대학교 전자공학과 박사과정 수료
1995 ~ 현재 전북과학 대학 인터넷 정보계열 교수